File Storage Policy

Document Reference: IT-POL-110

Document Classification: Policy

Data Classification: Public

Version number: 2.0

Relevant CIS Control(s): 3.9-3.11, 10.3, 10.4

Status: Approved

Approved by (Board): University Leadership Team

Approval date: 03 June 2025

Effective from: 03 June 2025

Review Frequency: Annual

Next review date: 03 June 2026

Document author: Cyber Security

Document owner: Director of Technology

Contact: IT Services

Collaborative provision: No

State whether this document is applicable to the University's collaborative partners

Related documents: Information Governance and Assurance Policy, Data Protection Policy, Information Security Controls Policy, Data Classification and Handling Policy, Acceptable Use Policy

University document: No

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: hull.ac.uk

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.
- This document is available in alternative formats from policy@hull.ac.uk.

File Storage Policy

Table of Contents

File Storage Policy

1 Introduction

1.1 This policy outlines the use of file storage within the University of Hull to protect *organisational data* from data breaches and cyber-attacks, for example.

1.2 This policy supports the objectives of the overarching **Information Governance and Assurance Policy**, **Information Security Controls Policy**, as well as the **Data Protection Policy**, **Data Breach Policy**, and the **Data Classification and Handling Policy**.

1.3 This policy should also be implemented in conjunction with the **Acceptable Use Policy**.

1.4 A glossary of technical terms, which are defined in pink, underlined, and italicised, can be found at the end of this policy. Clicking on each term will take you to its definition.

2 Scope

2.1 This policy, and all policies referenced herein, shall apply to all members of the University community, including faculty, students, administrators, staff, alumni, authorized guests, delegates, and independent contractors (the "End user(s)" or "you") who use the University's *IT Resources*.

2.2 This policy covers all *IT Resources* used to conduct University related business, and any authorised file storage methods used.

2.3 The University owns all data created by its employees unless it is created in a private capacity that is inconsequential to the employee's role. However, data that is created from research, which is paid for by an industry partner, sponsored or supported by an external funding source maybe exempt to this rule.

2.4 Data created by students during their studies or research will normally belong to the student, unless any of the following apply:

- The student receives a university studentship (a funded place on a programme), in which case ownership of the data will be decided in line with the terms of that studentship agreement.
- The student receives a bursary from, or have your fees paid or subsidised by, a sponsor, in which case the ownership of the data will be decided in line with the terms of the arrangement between the student, the University and the students sponsor.
- The data builds upon existing data created by the University or was jointly created by University employees or associates.
- The data builds upon existing data owned by a third party or was jointly created with a third party or University employees or associates.
- The student is an employee of the University and created the data in their role (in which

case, see 2.3 above).

3 Local (fixed) disk drives

3.1 Local (fixed) disk drives (aka 'C: drive') on managed devices are for the primary purpose of storing the operating system and local profile settings for users of the device. These should always be regarded as volatile – when a managed device is imaged it **will** overwrite any data on it.

3.2 Local (fixed) disk drives **must not** be used for any storage of University or personal data. University data should always be stored on University network storage or approved University cloud storage services.

3.3 Local (fixed) disk drives should not be considered as secure.

3.4 IT Services will reserve the right to refuse any request to attempt restoration of any University or personal data that has been lost by having been stored on local (fixed) disk drives.

4 University Network storage

4.1 IT Services provide centralised *network storage* for all University members that may be hosted in University data centres or in third-party 'cloud' facilities. Network storage is subject to regular backup with a retention period of 18 months.

4.2 *Network storage* provided by the University is secured by authentication and access control but not encrypted. This should be sufficient for business needs, however research data, for example, may need to be encrypted.

4.3 *Network storage* is subject to quotas and must only be used for storing University data, and not for the purpose of storing personal information such as photos, music, or videos.

4.4 A 'home' area is provided for individual use and can only be accessed by the member of the University that it is provisioned for.

4.5 Should a line manager require access to files held in a 'home' area that has been closed, they should submit an access request to the University Data Protection Officer. The request will be assessed and authorised in accordance with the University **Data Protection Policy.**

4.6 As per section 5 of this policy, IT Services recommend that organisational data is stored in the authorised cloud storage provider (OneDrive). Where shared collaboration routinely occurs, it is recommended that this is done via SharePoint – which should have a site created for each department. Please contact IT Services if a SharePoint site is required and does not yet exist.

4.7 If cloud storage is not suitable for the type of organisational data that is to be stored, a request must be made to IT Services via the Support Portal. When submitting a request of this nature, the following details must be included/agreed to:

- Who will be the designated owner.

This will either be the member requesting its creation, or a member to whom ownership has been transferred.

- Who else requires access to the shared storage area.
- Agree to comply with the University **Data Protection** and **Data Classification & Handling Policies** and accept their responsibilities for its ongoing management.
- Accept responsibility for ensuring access is restricted to only authorised university members or known third parties, Research Collaborators for example.

IT Services shall provide a suitable mechanism to allow the owner capability to administer group membership.

- Where a designated owner, or the line manager of that owner, needs to arrange cover for planned or unplanned absence, the owner or line manager should request temporary or permanent transfer of ownership or add an additional owner.

This can be requested through IT Services. An additional or temporary owner will have the same levels of responsibility for the area as the original, designated owner.

- If an end user assigned as owner changes role or leaves the institution, the line manager must ensure that ownership is transferred through a request to IT Services.
- Should a shared area owner be assigned in error, the owner should contact IT Services.

4.8 All owners will be notified on a quarterly basis to review the current membership of each shared area for which they have responsibility.

4.9 End users must notify the University Data Protection Officer (via the Support Portal) if they know or suspect that any data has been breached or if data is inappropriate for shared areas. Where personal identifiable information (PII) is involved, the procedures in the **Data Protection** and **Data Breach Policies** must be followed.

5 Cloud storage

5.1 Only University approved *cloud storage* services should be used for the storing of *organisational data*. Details of University approved and provided cloud storage services can be found on the University Support Portal.

5.2 All University approved *cloud storage* will be *encrypted* whilst at rest and in transit.

5.3 Most end users are eligible for a University approved *cloud storage* account. Details of eligibility can be found on the University Support Portal.

5.4 *Cloud storage* allows for collaborative working. When sharing files, it is the responsibility of the storage area owner to check that the files are being shared with the intended collaborators.

5.5 Caution should always be exercised when sharing files through public links. These are *not* restricted to University of Hull end users and anyone who is in possession of the link can access the shared files. This may not always be the intended recipient. To mitigate the risks of unintended sharing of files in this way IT Services have set the default expiry time of any shared public links to a period of 90 days.

5.6 If an end user changes role or leaves the institution and are an owner of files that have been previously shared, it is the responsibility of that member to ensure that ownership of files is transferred to another appropriate member before they do so.

5.7 When an end user leaves the institution or changes to a role which no longer entitles them to a cloud storage account, their cloud storage account will be closed and then deleted after a period of 30 days.

5.8 Should a line manager require access to files held in a cloud storage account that has been closed they should submit an access request to the University Data Protection Officer. The request will be assessed and authorised in accordance with the University **Data Protection Policy**.

5.9 Cloud storage is subject to quotas and must only be used for storing University data, and not for the purpose of personal information such as photos, music, or videos, as outlined in the **Acceptable Use Policy**.

5.10 Microsoft OneDrive, SharePoint and Exchange data is held within the UK whilst data for Teams is stored in the EU Zone.

5.11 If there is a need to store *PII* on University approved cloud storage, then this must be done in accordance with the University **Data Protection Policy**.

5.12 University members must notify the University Data Protection Officer (via the Support Portal) if they know or suspect that any University data has been breached when using our approved cloud storage. If *PII* is involved, the procedures in the University **Data Protection Policy** and **Data Breach Policies** must be followed.

6 Removable media

6.1 *Removable media* refers to any type of digital storage that is not physically fixed inside a device.

6.2 *Removable media* has many risks associated with its use, including:

- Providing a common route for the introduction of malware
- Accidental or deliberate export of sensitive data.

In the normal course of business, it should not be necessary to use removable media, and the risk of doing so usually outweighs any perceived benefit.

- Being very easy to lose, which can, and does, result in the breach of data.

- When used to transfer information from one device to another, for example a University PC to one at home, it can be utilised by attackers to transport malicious software from one environment to the other.

6.3 Whilst the use of *removable media* within the University is not prohibited, it should only be used in cases where no suitable alternative exists (e.g. Network storage, shared areas or cloud storage).

6.4 Managers and information asset owners shall ensure that use of *removable media* is suitably controlled within their area of responsibility in line with the objectives of this policy.

6.5 End users within professional services electing to use *removable media*, shall be responsible for ensuring they are authorised to do so within their area.

6.6 Any *removable media* used by staff to transport or store any *organisational data* should be purchased via approved channels.

6.7 Personally owned *removable media* shall not be used by staff for the purposes of transporting or storing University data.

6.8 Data on *removable media* must be encrypted. Guidance on *encryption* including recommended hardware and software shall be available to end users from the Support Portal.

6.9 Researchers are responsible for ensuring that use of *removable media* and the *encryption* of any such media meets the requirements imposed upon them by their research (e.g. by funders, or data sharing agreements).

6.10 Use of *removable media* by third parties or sub-contractors should be risk-assessed and authorised, and in accordance with University **Data Protection Policy** governing third-party access to data.

6.11 It is recommended that *removable media* be made externally identifiable where possible (e.g. using a fob/tag or to note the owners name/contact number).

6.12 When the *removable media* has reached the end of its useful life it should be submitted to IT Services for secure destruction.

6.13 If removable media has been lost, it should be reported to Data protection in line with the University **Data Breach Policy**.

6.14 If *removable media* has been found, it should be handed in to the Campus Security team. If identifiable (from a description/external labelling) then attempts will be made to return to its owner. If this is not the case, *removable media* must never be inserted into a device to try and identify its owner, as this can present a security risk.

6.15 Any unidentifiable *removable media* that has not been claimed within six months will be submitted for secure destruction.

7 Glossary of Terms

7.1 *Cloud Storage* = Storage that is kept at a different location and maintained by a third-party, who are responsible for managing the underlying infrastructure and ensuring the stored data is kept secure. The third-party ensures that access to cloud storage is always available, whether that is via a public or private internet connection. There are three different cloud storage models: 1) Public – the infrastructure that stores one organisation's data, is also used to store other organisations' data, and is spread across different geographical regions; 2) Private – an organisation uses dedicated infrastructure, provided by the third-party, and private connections help prevent unauthorised access to stored data; and 3) Hybrid – a combination of public and private models, which allows an organisation to decide what data to store where depending upon the data classification[1].

7.2 *Encryption* = The process of encoding a message or information in such a way that only authorized parties can access it[2]. This provides an additional level of security, even greater than that of a password, by scrambling a file, for example, so that they cannot be opened unless correctly *decrypted*. This is similar to the use of a lock and key, where the use of a pseudo-random encryption key is generated by an algorithm. Encryption itself does not prevent interference but does hide the actual content of a file from a would-be interceptor. Data can be encrypted whilst it is in its 'rest state' (i.e., stored on a disk), whilst it is being transmitted from one device to another, and whilst it is 'in use' (i.e., being processed)[3].

7.2.1 *Decryption* = The process of using a 'key' to unscramble information. An authorized recipient, who possesses the key (encryption algorithm), can easily decrypt the message with the key provided by the originator[4]. It is theoretically possible to decrypt the message without possessing the key, but considerable computational resources and skills are required to 'crack'.

[1] https://cloud.google.com/learn/what-is-cloud-storage
[2] https://www.cloudflare.com/learning/ssl/what-is-encryption/
[3] https://cloud.google.com/docs/security/encryption-in-transit
[4] https://www.techtarget.com/searchsecurity/definition/cryptography

7.3 *IT Resources* = Also known as an enterprise asset, these refer to a resource, owned by an enterprise (the University of Hull), with the potential to process or store data[5]. These include computing, networking, communications, application, and tele-communications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services. Figure 2, below, defines what is meant by an enterprise asset and provides examples – although it should be noted that this list is not exhaustive.

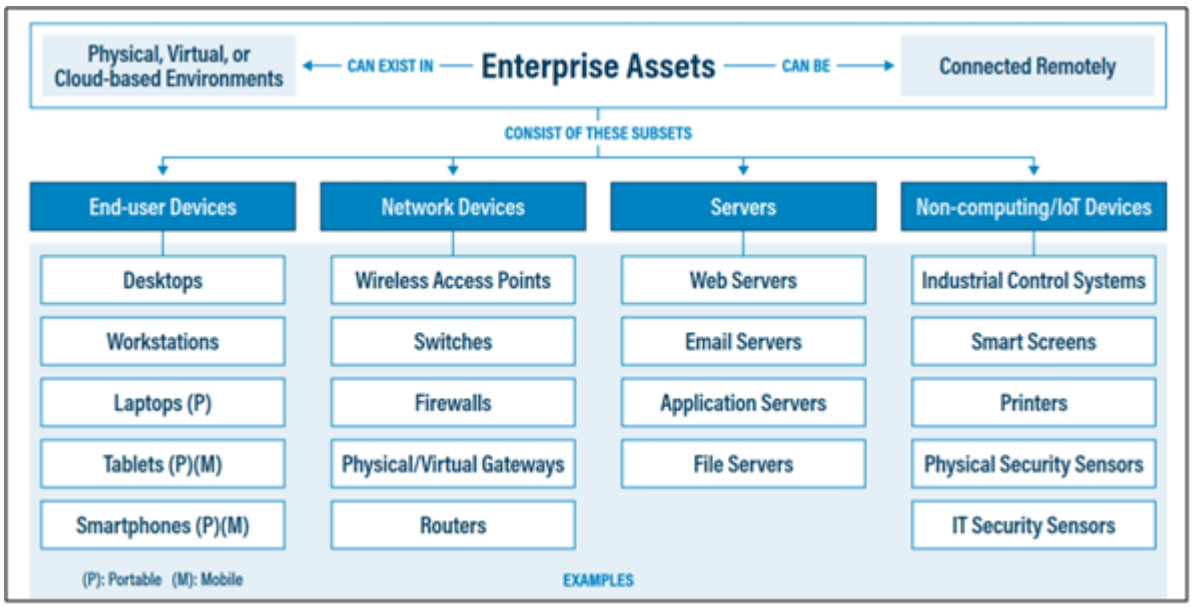

Figure 1: Enterprise Asset definition according to CIS Controls v8

7.4 *Network Storage* = Storage that is centralised and stored on campus, so it can be accessed over an *internal network* by many different end users[6]. This allows for collaboration and is different to cloud storage, which is usually accessed via a public network (the internet).

[5] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)
[6] https://www.techtarget.com/searchstorage/definition/network-attached-storage

7.4.1 *Internal Network* = Also known as a private or local area network (LAN)[7] or the intranet, the internal network has restricted access to only users who have been authorised to access it – for example, by the issuance of credentials (i.e., a university username/ email address and a password). This protects *organisational data* from being accessed by virtually anyone, as it allows for more granular controls and security measures, as well as being able to control network speed and congestion[8]. When working away from campus, access to the internal network, and therefore university resources, is usually required via a VPN.

7.5 *Organisational Data* = Data owned by the university; this can include any research data, office documents, financial data, and even email.

7.6 *Personal Identifiable Information (PII)* = Also known as 'personal data' PII refers to any information relating to an identified or identifiable person ('data subject'). An identifiable person is one who can be identified – directly or indirectly – by reference to an identifying characteristic; for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[9].

7.7 *Removable media* = A type of storage device that can easily be removed from a computer whilst it is still running. Removable media allows for the easy transference of data from one computer to another[10]. Examples of these devices include but is not limited to: USB flash drives (aka 'memory sticks', pens), external hard disk drives, phones using SD card storage, and optical media (e.g. DVD, CD). Given that these are easily portable and may not have built-in security measures, they can be subject to abuse and can introduce cyber security risks to the University network. If an end user finds any removable media, do not plug it in to a computer, but instead report it to Security and/or IT Services.

[7] https://purple.ai/blogs/whats-the-difference-between-a-lan-and-a-wan/
[8] https://www.digi.com/blog/post/private-network-vs-public-network
[9] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/
[10] https://www.techtarget.com/searchdatabackup/definition/removable-media

8 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

8.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[11]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[12]. A brief definition of each role is given in the table below.

8.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	IT Services
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Director of Technology
Consulted (C)	Provide input based on how this will impact their domain of expertise	Information Governance Committee
Informed (I)	Those who are kept up to date on progress	University Leadership Team

9 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Graeme Murphy	1 August 2023	All
2.0	Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All

[11] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[12] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/